

BUCHSTEINER LOOPS: ASSOCIATORS AND CONSTRUCTIONS

ALEŠ DRÁPAL AND MICHAEL KINYON

ABSTRACT. Let Q be a Buchsteiner loop. We describe the associator calculus in three variables, and show that $|Q| \geq 32$ if Q is not conjugacy closed. We also show that $|Q| \geq 64$ if there exists $x \in Q$ such that x^2 is not in the nucleus of Q . Furthermore, we describe a general construction that yields all proper Buchsteiner loops of order 32. Finally, we produce a Buchsteiner loop of order 128 that is nilpotency class 3 and possesses an abelian inner mapping group.

Buchsteiner loops are those loops that satisfy the Buchsteiner law

$$x \setminus (xy \cdot z) = (y \cdot zx) / x.$$

Their study was initiated by Hans Hoenig Buchsteiner [2]. His paper left many problems open, some of which were recently solved [8]. In particular we know now that the nucleus $N = N(Q)$ is a normal subloop of every Buchsteiner loop Q and that Q/N is an abelian group of exponent four.

Buchsteiner loops are closely connected to conjugacy closed loops (CC loops). A CC loop is conjugacy closed if and only if Q/N is a boolean group (i.e. a group of exponent two), by [9]. Not every Buchsteiner loop with Q/N boolean needs to be conjugacy closed (there are plenty of examples now. Some of them appear in this paper, and many other can be derived from the ring construction of [7].)

In every Buchsteiner loop Q the mappings $L_{xy}^{-1}L_xL_y$ and $R_{yx}^{-1}R_xR_y$ are automorphisms of Q , by [8], and this fact effects the behaviour of the associators $[x, y, z] = (x \cdot yz) \setminus (xy \cdot z)$. The group $Q/A(Q)$ acts upon $N = N(Q)$ (that always holds when Q/N is a group since then $A(Q) \leq Z(N(Q))$, by [10]. Here $A(Q)$ denotes the least normal subloop $A \trianglelefteq Q$ such that Q/A is a group. If Q/N is a group, then $A(Q)$ coincides with the subgroup generated by all associators $[x, y, z]$, by [11]). By translating the automorphism behaviour of $L_{xy}^{-1}L_xL_y$ into relations between associators we get that $[x, y, uv] = [x, y, u]^v[x, y, v]$ for all $x, y, u, v \in Q$. Note that n^v is defined as $v \setminus (nv)$, for all $v \in Q$ and $n \in N$.

If Q is a loop such that Q/N is a group, then one can code the Buchsteiner identity as

$$[x, y, z]^x = [y, z, x]^{-1} \text{ for all } x, y, z \in Q.$$

The cyclic shift expressed by this action implies that in every Buchsteiner loop we have

$$[x, y, uv] = [x, y, u]^v[x, y, v], [x, uv, y] = [x, u, y]^v[x, v, y], [uv, x, y] = [u, x, y]^v[v, x, y]$$

2000 *Mathematics Subject Classification.* Primary 20N05; Secondary 08A05.

Key words and phrases. Buchsteiner loop, conjugacy closed loop, associator, abelian inner mapping group.

The first author (A. Drápal) was supported by institutional grant MSM 0021620839 and by Grant Agency of Charles University, Grant 444/2004. This paper was written while he was a Fulbright Research Scholar at University of Wisconsin-Madison.

for all $x, y, u, v \in Q$. If Q/N is a group, then an associator $[x, y, z]$ depends only upon the ordered triple (xN, yN, zN) , by [10]. If Q is a Buchsteiner loop, then Q/N is an abelian group, and so we have $[x, y, uv] = [x, y, vu] = [x, y, v]^u [x, y, u] = [x, y, u][x, y, v]^u$. Similar relations clearly hold for the other two positions too. All the facts above are exposed in [8] in detail, and we shall use them freely in this paper.

In Section 1 we shall develop the associator calculus in three variations, building upon the identities that were established in [8]. Sections 2–4 are mainly concerned with the proof that proper Buchsteiner loops are of order at least 32 (by a *proper* Buchsteiner loop we understand a Buchsteiner loop that is not conjugacy closed). Buchsteiner loops Q such that Q/N is not boolean are necessarily proper, and for them we show that $|Q| \geq 64$. In Section 4 we will observe that nilpotent proper Buchsteiner loops have to be of nilpotency class at least 3, a result that appears also in [7].

In Section 6 we will show that a proper Buchsteiner loop of order 32 really exists, and that all such loops can be obtained by a general construction that doubles the size of a loop. This construction is described in Section 5. The starting loop must be a Buchsteiner loop, but not necessarily a proper one.

In a loop Q it is usual to denote by L_x the left translation $y \mapsto xy$, and by R_x the right translation $y \mapsto yx$. The permutation group generated by all L_x and R_x is known as the *multiplication group*, and the stabilizer of the unit is called the *inner mapping group*; we denote it by $\text{Inn } Q$. It is well known that $\text{Inn } Q$ is generated by all mappings $L(x, y) = L_{xy}^{-1} L_x L_y$, $R(x, y) = R_{yx}^{-1} R_x R_y$ and $T_x = R_x^{-1} L_x$. If Q is of nilpotency class two, then the inner mapping group is abelian, a result that goes back to Bruck [1]. The converse is not true, but the examples are not easy to find. Up to now there has been published only one example, by Csörgő [5]. Her example has 128 elements, was constructed indirectly by means of group transversals (see also [4]), and does not belong to any of known specific loop classes. In Sections 7 and 8 we construct a proper Buchsteiner loop Q of order 128 with $\text{Inn } Q$ abelian. This loop is different from the construction of [5], and is necessarily of nilpotency class three since the Buchsteiner loops of nilpotency class two are conjugacy closed. Section 7 is concerned with general properties of Buchsteiner loops that have abelian inner mapping groups, and Section 8 contains the construction. Note that (left) conjugacy closed loops with abelian inner mapping groups are always of nilpotency class at most two, by [3].

1. ASSOCIATOR IDENTITIES

Let Q be a Buchsteiner loop. Then $[z^{-1}, x, y]^{z^{-1}} = [x, y, z^{-1}]^{-1}$, which we write as $[x, y, z^{-1}]^z = [z^{-1}, x, y]^{-1}$. Therefore $1 = [x, y, z^{-1}z] = [x, y, z^{-1}]^z [x, y, z] = [z^{-1}, x, y]^{-1} [x, y, z]$. Hence $[x, y, z] = [z^{-1}, x, y]$. This identity comes from [8], where many further similar calculations have been performed. The next two lemmas give a selection of them.

Lemma 1.1. *Let Q be a Buchsteiner loop with elements x, y and z . Put $s = [x^2, y, z]$. Then $s = s^x = s^y = s^z$, $s^2 = 1$, and $s = [y, z, x^2] = [z, x^2, y]$. Furthermore, each of x^2, y^2 and z^2 centralizes $[x, y, z]$ (e.g. $[x, y, z]^{x^2} = [x, y, z]$ etc.).*

Lemma 1.2. *Let Q be a Buchsteiner loop with elements x, y and z . Put $u = [x, y^{-1}, z]$. Then:*

- (i) $[x, y, z]^2 = [y, z, x]^2 = [z, x, y]^2 = u^2$;
- (ii) $[x, y, z][y, z, x] = [z, x, y][x, y^{-1}, z]$;
- (iii) $u = [x, y^{-1}, z] = [y, z^{-1}, x] = [z, x^{-1}, y]$; and
- (iv) $u^x = [z, x, y]^{-1}$, $u^y = [x, y, z]^{-1}$, and $u^z = [z, x, y]^{-1}$.

The fact that Q/N is of exponent four, in every Buchsteiner loop Q , means that $[x^4, y, z] = 1$ and $[x^{-1}, y, z] = [x^3, y, z] = [x^2, y, z][x, y, z]$, for all $x, y, z \in Q$.

Proposition 1.3. *Let Q be a Buchsteiner loop with elements x, y and z . Put $u = [x, y^{-1}, z]$, $s_x = [x^2, y, z]$, $s_y = [y^2, z, x]$ and $s_z = [z^2, y, x]$. Then $s_x = u^x u$, $s_y = u^y u$ and $s_z = u^z u$. Furthermore,*

$$s_x s_y s_z = 1, \quad u^x u^y u^z = u^{-3}, \quad u^{xyz} = u^{-1}, \quad \text{and} \quad (u^2)^x = (u^2)^y = (u^2)^z = u^{-2}.$$

Proof. Each of s_x , s_y and s_z is of exponent two, and $[z, x, y]^{x^2} = [z, x, y]$, by Lemma 1.1. From points (iii) and (iv) of Lemma 1.2 we can compute $u^x u$ as $[z, x^{-1}, y]^x [z, x^{-1}, y] = [z, x, y]^{-1} [z, x, y] [z, x^2, y] = s_x$, and the identities $u^y u = s_y$ and $u^z u = s_z$ can be proved similarly. Points (i) and (iv) of Lemma 1.2 yield $(u^2)^x = (u^2)^y = (u^2)^z = u^{-2}$. Point (ii) of the lemma can be written as $1 = u^y u^z (u^x)^{-1} u$, and $(u^x)^{-1}$ can be replaced by $(u^x)(u^x)^{-2} = u^x u^2$. This means $u^x u^y u^z = u^{-3}$, and so $s_x s_y s_z = u^x u u^y u u^z u = 1$. Finally, $u^{xyz} = u^{y x z} = ([x, y, z]^{-1})^{x z} = [y, z, x]^z = [y, z^{-1}, x]^{-1} = u^{-1}$ (recall that z^2 centralizes $[y, z, x]$, by Lemma 1.1). \square

Note that $[x, y, z]^{xy} = ([y, z, x]^{-1})^y = [z, x, y]$, for all $x, y, z \in Q$. This gives $[x, x, y] = [x, x, y]^{x^2} = [y, x, x]$. We shall now prove some further facts that involve only two variables. Most of the equalities can be found in [8], but we shall prove them here, in order to keep the interface with [8] limited. (There are usually many ways how one can obtain an identity. Proposition 1.3 can be always used when an associator is conjugated by a composition of its arguments. So we can also get $[x, y, z]^{xy}$ as $(u^{-1})^{yxy} = (u^{-1})^x = [z, x, y]$.)

Lemma 1.4. *Let Q be a Buchsteiner loop with elements x and y . Put $u = [x, y, x]$ and $v = [x, x, y]$. Then*

$$u^y = u^{-1}, \quad v^y = v^{-1}, \quad u^x = v^{-1}, \quad v^x = u^{-1}, \\ u^2 = v^2 = [y, x, y]^2 = [y, y, x]^2 \quad \text{and} \quad uv^{-1} = vu^{-1} = [x^2, x, y].$$

Furthermore, $[x, y^2, x] = 1$ and $[x, x, x]^y = [x, x, x](uv)^{-1}$.

Proof. We have $[x, y^2, x] = [y^2, x, x]$, by Lemma 1.1, and $[y^2, x, x]$ is equal to $[y, x, x]^y [y, x, x] = [x, x, y]^{-1} [y, x, x] = 1$. Hence $u = [x, y^{-1}, x] = [x, y, x][x, y^2, x]$, and the equalities $u^y = u^{-1}$ and $u^x = v^{-1}$ follow from Proposition 1.3. By Lemma 1.1, $u^2 = v^2$ (and so $uv^{-1} = vu^{-1}$), and both of u and v are centralized by both of x^2 and y^2 . Thus $u^x = v^{-1}$ yields $v^x = u^{-1}$. Clearly, $[x^2, x, y] = v^x v = u^{-1} v$, and $v[x, x, x]^y = [x, x, xy] = [x, x, x]v^x = [x, x, x]u^{-1}$. A similar argument can be used to prove $[y, x, y]^2 = v^2$. Indeed,

$$[y, x, y]v^{-1} = [y, x, y]v^y = [yx, x, y] = v[y, x, y]^x = v[y, x, y]^{-1}.$$

\square

More results can be obtained by arguments similar to the one we used when computing $[x, x, x]^y$:

Lemma 1.5. *Let Q be a Buchsteiner loop with elements x, y and z . Then:*

$$\begin{aligned} [x, y, x]^{z^2} &= [x, y, x], \quad [x, x, y]^{z^2} = [x, x, y], \quad [x^2, x, y]^z = [x^2, x, y] \quad \text{and} \\ [x, y, x]^z &= [x, y, x][x^2, y, z][z, x, y]^{-2} = [x, y, x][x^2, z, y][z, y, x]^{-2}. \end{aligned}$$

Proof. Write $[xz^2, x, y]$ as $[x, x, y]^{z^2}[z^2, x, y]$ and as $[x, x, y][z^2, x, y]^x$. We know that x centralizes $[z^2, x, y]$, by Lemma 1.1, and hence z^2 centralizes $[x, x, y]$. A similar argument shows that z^2 also centralizes $[x, y, x]$. Furthermore, $[x^2, x, y][z, x, y] = [x^2, x, y][z, x, y]^{x^2} = [x^2z, x, y] = [x^2, x, y]^z[z, x, y]$, and so z centralizes $[x^2, x, y]$.

Write $[xz, x, y]$ as $[x, x, y]^z[z, x, y]$ and as $[x, x, y][z, x, y]^x = [x, x, y][z, x^{-1}, y]^{-1}$. Hence $[x, x, y]^z = [x, x, y]v$, where $v = [z, x^{-1}, y]^{-1}[z, x, y]^{-1} = [z, x^2, y][z, x, y]^{-2}$, and so $[x, y, x]^z = ([x, x, y][x^2, x, y])^z = [x, x, y][x^2, x, y]v = [x, y, x]v$, by the preceding parts of the proof and by Lemma 1.4.

Proceeding similarly, write $[xz, y, x]$ as $[x, y, x]^z[z, y, x]$ and as $[x, y, x][z, y, x]^x = [x, y, x][x, z, y]^{-1}$. Thus $[x, y, x]^z = [x, y, x]w^{-1}$, where $w = [z, y, x][x, z, y] = [y, x, z][y, x^{-1}, z] = [y, x^2, z][y, x, z]^2$, by points (ii) and (iii) of Lemma 1.2. \square

To make complete our understanding of the associator calculus in three variables we need to establish the relationship of associators $[x, y, z]$ and $[y, x, z]$.

Proposition 1.6. *Let Q be a Buchsteiner loop with elements x, y and z . Then*

$$[x, y, z][z, y, x]^{-1} = [y, z, x][x, z, y]^{-1} = [z, x, y][y, x, z]^{-1}.$$

Denote this element by a , and put $s_x = [x^2, y, z]$, $s_y = [y^2, z, x]$ and $s_z = [z^2, y, x]$. Then

$$\begin{aligned} a^2 &= 1, \quad a^x = a^y = a^z = a, \quad [x, y, z]^2 = [x, z, y]^2, \quad [x^2, y, z] = [x^2, z, y], \quad \text{and} \\ [x, y, z][x, z, y]^{-1} &= as_x = [y, z, x][z, y, x]^{-1} \\ [y, z, x][y, x, z]^{-1} &= as_y = [z, x, y][x, z, y]^{-1} \quad \text{and} \\ [z, x, y][z, y, x]^{-1} &= as_z = [x, y, z][y, x, z]^{-1}. \end{aligned}$$

Proof. We shall again use the equality $[x, y, z]^{xy} = [z, x, y]$. We obtain:

$$\begin{aligned} [xy, xy, z] &= [x, xy, z]^y[y, xy, z] = [x, x, z]^y[x, y, z]^{xy}[y, y, z]^x[y, x, z] = \\ &= [x, x, z]^y[y, y, z]^x[z, x, y][y, x, z], \quad \text{and} \\ [xy, xy, z] &= [x, xy, z][y, xy, z]^x = [x, x, z]^y[x, y, z][y, y, z]^x[y, x, z]^{yx} = \\ &= [x, x, z]^y[y, y, z]^x[x, y, z][z, y, x]. \end{aligned}$$

By comparing the right hand sides we get $[x, y, z][y, x, z]^{-1} = [z, x, y][z, y, x]^{-1}$. We also have $[x, y, z][y, x, z] = [z, x, y][z, y, x]$, since $[y, x, z]^2 = [z, y, x]^2$, by point (i) of Lemma 1.2. Therefore,

$$[x, y, z][z, y, x]^{-1} = [z, x, y][y, x, z]^{-1} = [y, z, x][x, z, y]^{-1},$$

where the latter equality is an instance of the former one. Denote this element by a , as in the text of the proposition. Note that we have proved that the leftmost term and the rightmost term coincide in all three last equalities of the proposition.

Now, $[x^2, y, z] = [x, y, z][x, y, z]^2 = [x, y, z][y, z, x]^{-1}$ equals $[z, y, x][x, z, y]^{-1} = [z, y, x^2] = [x^2, z, y]$, and that immediately yields $[x, y, z]^2 = [z, x, y]^2 = [z, y, x]^2 = [x, z, y]^2$, by Lemma 1.5 and by point (i) of Lemma 1.2. Therefore $a^2 = 1$, and $a^x = [z, x^{-1}, y]^{-1}[y, x^{-1}, z] = a^{-1}[z, x^2, y]^{-1}[y, x^2, z] = a^{-1} = a$. Similarly, $a^y = a$

and $a^z = a$. Finally, $[x, y, z][x, z, y]^{-1} = [x, y, z][y, z, x]^{-1}a = a[x, y, z][x, y, z]^x = a[x^2, y, z] = as_x$. \square

We finish this section by an easy (but handy) observation:

Lemma 1.7. *Let Q be a Buchsteiner loop with elements x, y and z . If $[x, y, z] = 1$, then $[y, z, x] = [z, x, y] = 1$ as well.*

Proof. Use equalities $[x, y, z]^x = [y, z, x]^{-1}$ and $[x, y, z]^{xy} = [z, x, y]$. \square

2. CENTRAL ELEMENTS AND AN ODD ORDER PROPOSITION

As we have already hinted in the introduction, Buchsteiner loops are closely connected to conjugacy closedness. By [11], a loop Q is conjugacy closed if and only if Q/N is an abelian group and all associators are invariant under every permutation of their arguments. If we assume that Q/N is a boolean group, then the condition for Buchsteiner identity is a natural weakening of the condition for the conjugacy closedness. Indeed, if Q/N is a boolean group, then Q is a Buchsteiner loop if and only if $[x, y, z] = [y, z, x]$ for all $x, y, z \in Q$, i. e. if the associators are invariant under the cyclic shifts, by [7] (see also Lemma 4.6).

By [6], if Q is a Buchsteiner loop, then $Q/Z(Q)$ is a conjugacy closed loop.

Proposition 2.1. *Let Q be a Buchsteiner loop with elements x, y and z . Then $[x, y, z][x, z, y]^{-1} = [x, y, z][y, x, z]^{-1}$, $[x, y, z][z, y, x]^{-1}$, and $[x^2, y, z] = [y, z, x^2] = [z, x^2, y]$ are central elements of exponent 2, and $[x, y, z]^{u^2} = [x, y, z]$ for each $u \in Q$.*

Proof. Since the associators of a CC loop are invariant to permutations of arguments, there must be $[x, y, z] \equiv [x, z, y]$ and $[x, y, z] \equiv [z, y, x] \pmod{Z(Q)}$, and so the initial claims follow from Proposition 1.6. Since $Q/Z(Q)$ is a conjugacy closed Buchsteiner loop, each square element belongs to the nucleus of $Q/Z(Q)$. Associators that involve a nuclear element are trivial. Hence $[x^2, y, z] \equiv 1 \pmod{Z(Q)}$, and so $[x^2, y, z] \in Z(Q)$. Furthermore, $1 = [x^4, y, z] = [x^2, y, z]^{x^2}[x^2, y, z] = ([x^2, y, z])^2$, $[z, x^2, y]^z = [x^2, y, z]^{-1} = [x^2, y, z]$ and $[y, z, x^2]^y = [z, x^2, y]$. The last equality follows from expressing $[xu^2, y, z]$ both as $[x, y, z]^{u^2}[u^2, y, z]$ and as $[x, y, z][u^2, y, z]^x = [x, y, z][u^2y, z]$. \square

Note that Lemma 1.1 is a special case of Proposition 2.1. Methods of Section 1 suffice to prove Proposition 2.1 in Buchsteiner loops that are generated by three elements, but it is an open question if these methods can be used to prove Proposition 2.1 in the full generality. To formalize this problem consider a first order theory that involves a group $G \cong Q/A$, $A = A(Q)$, that acts upon a group N , and a ternary mapping $[-, -, -] : G^3 \rightarrow A \leq Z(N)$. In this theory we assume that $[x, y, zu] = [x, y, z]^u[x, y, u]$ and $[x, y, z]^x = [y, z, x]^{-1}$ for all $x, y, z, u \in G$, and that N/A can be identified with a subgroup $H \leq G$ in such a way that $[-, -, -]$ depends only upon classes modulo H , and G/H is an abelian group of exponent four.

The associator calculus developed in [8] (which is an earlier paper than [6]) can be formulated within such a theory, and this is also true for results of Section 1. The main results of this paper are independent of Proposition 2.1 since for them it suffices to know the statement only for 3-generated groups.

For a commutative group G denote by $O(G)$ the subgroup consisting of all elements of an odd order. If a loop Q contains a normal subloop H which is a group,

then every characteristic subgroup of H is clearly also a normal subloop of Q . In particular, if $A(Q)$ is abelian, then $O(A(Q)) \leq Q$.

We have already mentioned that if a loop Q is modulo the nucleus an abelian group, then it is conjugacy closed if and only if each $[x, y, z]$ does not depend on the order of the arguments. To verify the latter property it suffices to show $[x, y, z] = [y, x, z]$ and $[x, y, z] = [x, z, y]$, for all $x, y, z \in Q$.

Proposition 2.2. *Let Q be a Buchsteiner loop that is not conjugacy closed. Then neither $Q/O(A(Q))$ is conjugacy closed.*

Proof. We have $a = [x, y, z][y, x, z]^{-1} = [z, x, y][z, y, x]^{-1}$, by Proposition 1.6, and so our assumption implies the existence of $x, y, z \in Q$ such that $a \neq 1$. But then a is an involution, again by Proposition 1.6, and hence $a \notin O(A(Q))$. \square

Lemma 2.3. *Let Q be a Buchsteiner loop generated by a set X . If $[x, y, z] = [x, z, y]$ for all $x, y, z \in X$, then Q is a conjugacy closed loop.*

Proof. We need to prove $[t_2, t_1, t_3] = [t_1, t_2, t_3] = [t_1, t_3, t_2]$ for all $t_i \in Q$, $1 \leq i \leq 3$. Since Q is assumed to be a Buchsteiner loop, it suffices to prove only the latter identity. Indeed, If $[t_3, t_1, t_2] = [t_3, t_2, t_1]$, then $[t_1, t_2, t_3] = ([t_3, t_1, t_2]^{-1})^{t_3} = (([t_3, t_2, t_1]^{-1})^{t_3}) = [t_2, t_1, t_3]$. The elements $t_i \in Q$ can be regarded as terms in an abelian group of exponent 4, for which X is a set of generators. Each t_i has thus a length $|t_i| \leq 3|X|$, and we can proceed by induction along $s = \sum |t_i|$. The case $s = 3$ is a consequence of our starting assumption. Let us have $s \geq 4$. Then one of t_i , say t_2 is of the form uv . Using the induction assumption we get $[t_1, uv, t_3] = [t_1, u, t_3]^v [t_1, v, t_3] = [t_1, t_3, u]^v [t_1, t_3, v] = [t_1, t_3, uv]$. \square

Corollary 2.4. *Let Q be a Buchsteiner loop generated by x and y . Suppose that Q is not conjugacy closed. Then $[x, x, y] \neq [x, y, x]$ or $[y, y, x] \neq [y, x, y]$.*

Proof. If $[x, x, y] = [x, y, x]$ and $[y, y, x] = [y, x, y]$, then Q is conjugacy closed, by Lemma 2.3 with $X = \{x, y\}$. \square

Corollary 2.5. *Let Q be a Buchsteiner loop generated by a set X . Let Q_1 be the subloop generated by $X \setminus N$. If Q_1 is conjugacy closed, then Q is conjugacy closed as well.*

Proof. This follows from Lemma 2.3 too, since $[x, y, z] = 1 = [x, z, y]$ whenever $N \cap \{x, y, z\} \neq \emptyset$. \square

3. LOOPS THAT ARE NOT BOOLEAN MODULO THE NUCLUES

Lemma 3.1. *Let Q be a Buchsteiner loop with elements x, y and z . If $y^2 \in N(Q)$ and $z^2 \in N(Q)$, then $[x^2, y, z] = [y, z, x^2] = [z, x^2, y] = 1$.*

Proof. Both $[y^2, z, x]$ and $[z^2, y, x]$ are trivial, by our assumptions. From Proposition 1.3 we get $1 = [x^2, y, z][y^2, z, x][z^2, y, x] = [x^2, y, z]$. The cyclic shifts of the latter associator are trivial by Lemma 1.7. \square

Lemma 3.2. *Let Q be a Buchsteiner loop such that Q/N contains exactly one nontrivial square element x^2N . Then there exists $y \in Q$ such that $[x^2, x, y] \neq 1$, $y \notin xN$ and $y^2 \in N$.*

Proof. If $[x^2, x, y] \neq 1$, then $y \equiv x \pmod{N}$ since $[x^2, x, x] = 1$, by Lemmas 1.1 and 1.4, and there must be $y^2 \in N$, by the assumption of the unique square of Q/N . Therefore it suffices to find $y \in Q$ with $[x^2, x, y] \neq 1$.

The element x^2 does not belong to N , and hence $[x^2, y, z] \neq 1$ for some $y, z \in Q$. However, that means that at least one of y^2 and z^2 does not belong to N , by Lemma 3.1. We can assume $z^2 \notin N$, since $[x^2, y, z] = [x^2, z, y]$, by Proposition 1.6. If also $y^2 \notin N$, then $y \equiv xu \pmod{N}$ for some $u \in Q$ with $u^2 = 1$. In such a case $[x^2, y, z] = [x^2, xu, z] = [x^2, x, z]^u [x^2, u, z]$, and we are done if $[x^2, x, z] \neq 1$. Let us have $[x^2, x, z] = 1$. Then we are back to the case $[x^2, y, z] \neq 1$, but now we can assume that $y^2 \in N$. We know that $z \equiv xv$ for some $v \in Q$ with $v^2 \in N$ since $z^2 \notin N$, and there is a unique nontrivial square in Q/N . We have $[x^2, y, v] = 1$, by Lemma 3.1, and so $1 \neq [x^2, y, z] = [x^2, y, x] = [x^2, x, y]$. The last equality follows from Lemma 1.1. \square

Proposition 3.3. *Let Q be a Buchsteiner loop generated by elements x and y . Suppose that $[x, x, y] \neq [x, y, x]$. Then $[x^2, x, y] \neq 1$, $|Q/N| \geq 8$ and $|A(Q)| \geq 8$.*

Proof. The equalities established in Lemma 1.4 will be used freely throughout the proof. Put $a = [x^2, x, y] = [x, x, y][x, y, x]^{-1}$. We assume that $a \neq 1$, and therefore $|Q/N|$ is not of exponent two. $|Q/N|$ cannot be cyclic, since $[x^2, x, x] = 1$, and thus $|Q/N| \geq 8$. Now, $a^2 = 1$, by Lemma 1.1, and so $Q/O(A(Q))$ satisfies the hypothesis (cf. Proposition 2.2). We can hence assume that $A(Q)$ is a 2-group. Set $u = [x, y, x]$. Then $u \neq a$ since $1 \neq [x, x, y]^{-1} = u^x$. If $|u|$, the order of u , is greater than four, then $|A(Q)| \geq 8$. Assume $|u| = 4$. If $a \neq u^2$, then a and u generate a subgroup of order 8. Assume $a = u^2$. Then $u^x = [x, x, y]^{-1} = (ua)^{-1} = u^{-1}a = uau^{-2} = u$, and so to prove $|A(Q)| > 4$ it suffices to find an element $m \in A(Q)$ with $m^x \neq m$. Set $m = [x, y, x][y, x, y]^{-1}$. Then $m^x = [x, x, y]^{-1}[y, x, y] = am^{-1}$, and $m^{-1} = m$ as $[x, y, x]^2 = [y, x, y]^2$.

It remains to consider the case when u is an involution. In such a case $u^y = u$. The element a is central, by Lemma 1.1, and so to show $|A(Q)| > 4$ it suffices to find $s \in A(Q)$ with $s^y \neq s$. Set $s = [x, x, x]$. Then $s^y = s[x, x, y]^{-1}[x, y, x]^{-1}$, which equals sa since both $[x, x, y]$ and $[x, y, x]$ are assumed to be involutions. \square

The above proof can be seen as a starting point for constructing Buchsteiner loops of order 64 that are not boolean modulo the nucleus. As we prove below, 64 is the least order for such a loop. An example was constructed in [8], and one can hope that all such loops of 64 will be classified in future. The overlap of Proposition 3.3 and the ensuing Lemma 3.4 should be understood as justified by this intention.

Lemma 3.4. *Let x, y and z be such elements of a Buchsteiner loop Q that satisfy $[x^2, y, z] \neq 1$. Then $|A(Q)| \geq 8$.*

Proof. Set $s = [x^2, y, z]$. This is a central involution, and hence $Q/O(A(Q))$ satisfies the hypothesis, and we can assume that $A(Q)$ is a 2-group. Set $u = [x, y^{-1}, z]$ and note that $s = u^x u$, by Proposition 1.3. Therefore $u \neq 1$ and $u \neq s$. If $|u| \geq 8$, then we are done. Let us have $s = u^2$. Then $u^x = u$, and so $|A(Q)| \geq 8$

if we find $v \in A(Q)$ with $v^x \neq v$. Suppose that no such v exists. By considering the formula of Lemma 1.5 for $[y, z, y]^x$ and $[z, y, z]^x$, we get $[y^2, z, x] = [z^2, x, y] = u^2$, by point (i) of Lemma 1.2 (and by Proposition 1.6). Of course, $[x^2, y, z] = [x, y, z]^2 = u^2$ as well. From Proposition 1.3 we now obtain $1 = (u^2)^3 = u^2$, a contradiction.

It remains to consider the situation when $u^2 = 1$ and $|A(Q)| = 4$. Then $u^x = us$, and each of $u^y, u^z \in \{u, us\}$ since the element s is central. We cannot have both u^y and u^z equal to us because then $u^x u^y u^z = us \neq u$, and that contradicts Proposition 1.3.

Assume $u^y = u$. Then it suffices to find an element $v \in A(Q)$ with $v^y \neq v$. By Lemma 1.5, $[x, z, x]^y = [x, z, x]s$ since $[y, z, x]^2 = 1$ by Lemma 1.2, and so one can set $v = [x, z, x]$. The case $u^z = u$ is nearly the same. \square

Corollary 3.5. *Let Q be a Buchsteiner loop such that $Q/N(Q)$ is not a boolean group. Then $|A(Q)| \geq 8$ and $|Q : N(Q)| \geq 8$. If $|Q| = 64$, the $|A(Q)| = 8$ and $Q/N(Q) \cong C_4 \times C_2$.*

Proof. Since Q/N is not boolean, there must exist elements $x, y, z \in Q$ that satisfy the hypothesis of Lemma 3.4. Hence $|A(Q)| \geq 8$, and so Q/N has to be generated by at most two elements if $|Q| \leq 64$. In such a case we can assume that Q is generated by two elements, by Corollary 2.5, and we can also assume that $[x, x, y] \neq [x, y, x]$, by Corollary 2.4. The inequality $|Q : N|$ now follows from Proposition 3.3 (or directly from Lemma 3.2). \square

For future references we also record this in a somewhat less explicit way:

Corollary 3.6. *Let Q be a Buchsteiner loop such that Q/N is generated by less than three elements. If Q is not conjugacy closed, then $|Q/N| \geq 8$ and $|A(Q)| \geq 8$.*

4. COMMUTATOR CALCULUS AND LOOPS OF SMALL ORDER

Let x and y be elements of a loop Q . The commutator $[x, y]$ is defined by $yx[x, y] = xy$. Assume that $N = N(Q) \trianglelefteq Q$ and that Q/N is an abelian group. Then $xy = yx[x, y]^{-1}$ and so $[y, x] = [x, y]^{-1}$, as in groups. Furthermore, if Q/N is an abelian group, then one can connect associators and commutators by the formula

$$[xy, z] = [x, z]^y [y, z] [x, z, y]^{-1} [x, y, z] [z, x, y].$$

The proof is not difficult, and can be found, e. g., in [8].

Lemma 4.1. *Let Q be a Buchsteiner loop with elements x, y and z . Set $m = [z, x, y][z, y, x]^{-1}$. Then $m^2 = 1$, $m \in Z(Q)$,*

$$[xy, z] = [x, z]^y [y, z] [y, z, x] m \text{ and } [yx, z] = [y, z]^x [x, z] [x, z, y] m.$$

Proof. By Proposition 1.6 we can replace in the above formula the product $[x, z, y]^{-1} [x, y, z]$ with the product $[y, z, x] [z, y, x]^{-1}$. That gives the required expression of $[xy, z]$, and the expression of $[yx, z]$ uses the fact that m is a (central) element of exponent two, by Proposition 2.1. \square

We shall apply Lemma 4.1 to various situations, starting with cases that naturally imply $[y, z, x] = [x, z, y]$. The following observation be useful.

Lemma 4.2. *Let x, y and z be elements of a Buchsteiner loop Q such that $[x, y, z]$ is centralized by each of x, y and z . Then $[x, y, z] = [y, z, x] = [z, x, y]$ is of exponent two, and $[x^2, y, z] = [y^2, z, x] = [z^2, x, y] = 1$.*

Proof. Use the notation of Proposition 1.3. We see that $u = [x, y^{-1}, z]$ satisfies both $u^4 = 1$ and $u^6 = 1$ since we assume $u^x = u^y = u^z = u$, and $u^2 = [x, y, z]^2 = s_y$ is of exponent two, by Lemma 1.1. Hence $u^2 = 1$, and elements s_x, s_y and s_z are equal to 1. \square

Proposition 4.3. *Let Q be a Buchsteiner loop with elements x, y and z such that all elements $[x, y]$, $[y, z]$ and $[x, z]$ are central. Then $[x, y, z] = [y, x, z]$.*

Proof. First note that $[xy, z] = [yx, z]$ since $xy = yx[x, y]$ and we assume $[x, y] \in Z(Q)$. The rest follows from Lemma 4.1. \square

Corollary 4.4. *Let Q be a Buchsteiner loop of nilpotency class two. Then Q has to be conjugacy closed.*

Proof. The assumptions of both Lemma 4.2 and Proposition 4.3 are satisfied by all $x, y, z \in Q$, and so we see that the value of an associator does not depend upon the order of its arguments. \square

Corollary 4.5. *Let Q be a Buchsteiner loop such that $N(Q) \leq Z(Q)$. Then Q has to be conjugacy closed.*

Proof. Such a loop is necessarily of nilpotency class at most two. \square

Lemma 4.6. *Let Q be a Buchsteiner loop such that Q/N is a boolean group. Then*

$$[x, y, z] = [y, z, x] = [z, x, y] = [x, y^{-1}, z] \text{ for all } x, y, z \in Q.$$

Furthermore, $[x, y, z]^x = [x, y, z]^y = [y, z, x]^z = [x, y, z]^{-1}$.

Proof. This follows directly from Lemma 1.2 and Proposition 1.3. \square

Proposition 4.7. *Let Q be a Buchsteiner loop such that $|A(Q)| > 2$ and Q/N is a boolean group. If Q is not conjugacy closed, then $|Q| \geq 64$.*

Proof. Throughout the proof we shall be assuming that Q is not conjugacy closed. Thus $|Q : N(Q)| \geq 8$, by Corollary 2.5, Corollary 2.4 and Lemma 1.4. There cannot be $|N(Q)| = 2$, since otherwise $N(Q)$ would be central, and Corollary 4.5 would apply. We also know that $|A(Q)|$ is even, by Proposition 2.2. Choose $x, y, z \in Q$ such that $[x, y, z] \neq 1$ and $[x, z, y] \neq [x, y, z]$, and denote by Q_1 the loop generated by x, y and z . If $A(Q_1)$ has only two elements, then there must be $|Q : N(Q)| \geq 16$, and so $|Q| \geq 4 \cdot 16 = 64$. We can hence assume $Q = Q_1$.

Our goal is to show that there must be $|N(Q)| \geq 8$. Assume the contrary. If $|N(Q)| = 2$, then $N(Q) \leq Z(Q)$, and Q is a CC loop, by Corollary 4.5. If $A(Q) = N(Q)$ is of order 6, then we obtain the same kind of contradiction, by Proposition 2.2, and so $N(Q) = A(Q)$ has to consist of four elements, and not all of them can be central.

Assume first that $A(Q)$ is a boolean group. To obtain a contradiction, we shall show that $A(Q) \leq Z(Q)$. For that it suffices to prove $[u, v, w] \in Z(Q)$ for all

possibilities when $u, v, w \in \{x, y, z\}$, since the further cases follow from the associator multiplicative formula. Now, if $\{u, v, w\} = \{x, y, z\}$, then $[u, v, w] \in Z(Q)$ by Lemma 4.6. Furthermore, $[u, v, u]^w = [u, v, u]$, by Lemma 1.5, and the rest follows from Lemma 1.4 in a clear way.

Let now $N(Q) = A(Q)$ be a cyclic group of order four. Denote by b be the only nontrivial central element of Q . If $v \in Q$, then $v^2 \in N(Q)$. If $v^2 \in Z(Q)$, then $[v, v, v] = [v^2, v] = 1$. Consider an element $v \in Q$ with $[v, v, v] \neq 1$. Then $u = v^2$ has to generate $N(Q)$, and $[v, v, v] = [v^2, v]$ is equal to $u^{-1}u^v$. Thus v has to induce the (only admissible) nontrivial automorphism of $N(Q)$, and so $u^v = u^{-1}$. That means $[v, v, v] = b$, and so $[v, v, v] \in Z(Q) = \{1, b\}$ for all $v \in Q$.

Consider elements $v, w \in Q$. We have $[v, v, v] = [v, v, v]^w$, and the latter element is equal to $[v, v, v][v, w, v]^2$, by Lemma 1.4. Thus $[v, w, v]^2 = 1$ for all $v, w \in Q$, which in our situation means $[v, w, v] \in Z(Q)$.

To get a contradiction we shall prove now that $[u, v, w] \in Z(Q)$ for all $u, v, w \in Q$. This follows from Lemma 1.5 since from that lemma we see that $[u, v, w]^2 = 1$ for all $u, v, w \in Q$. \square

Proposition 4.8. *Let Q be a Buchsteiner loop of order less than 64 that is not conjugacy closed. Then $|Q| = 32$, Q/N is elementary abelian of order 8, and $Z(Q) = A(Q)$ is of order 2. The group $Q/Z(Q)$ is a nonabelian group of order 16.*

Proof. From Corollary 3.6 we know that Q/N has to be of order at least 8, and from Corollary 3.5 we know that it has to be elementary abelian. Furthermore $|A(Q)| = 2$, by Proposition 4.7. Thus $A(Q) \leq Z(Q)$, and there cannot be $A(Q) = N(Q)$, by Corollary 4.5. This means that $|Q : N| = 8$ and $|N| = 4$. From Corollary 4.5 we also see that $Z(Q)$ has to coincide with $N(Q)$. Finally, $Q/Z(Q)$ cannot be abelian, by Corollary 4.4. \square

5. THE DOUBLING CONSTRUCTION

The purpose of this section is to describe a construction based upon a Buchsteiner loop Q that produces a Buchsteiner loop P that contains the loop Q as a subloop of index two. It may happen that Q is a CC loop, while P is not, and in the next section we shall see that all proper Buchsteiner loops of order 32 can be obtained in this way.

Proposition 5.1. *Let P be a Buchsteiner loop with a normal subloop Q , where $|P : Q| = 2$. Let $z \in P \setminus Q$ be an element such that $d = z^2 \in N(P)$ and such that $q(u) = [z, u]$ belongs to $Z(Q)$ and is of exponent two for all $u \in Q$. Then:*

- (i) $[u, v, z] = [v, z, u] = [z, u, v] = q(vu)q(u)q(v) \in Z(P)$ for all $u, v \in Q$;
- (ii) $[z, z, z] = q(d) \in Z(P)$;
- (iii) $[u, z, z] = [z, u, z] = [z, z, u] = [d, u] = [u, d] \in Z(P)$.

Proof. We assume $[z, u]^2 = 1$, and hence $q(u) = [u, z] = [z, u]$ for all $u \in Q$. Consider $u, v \in Q$. Then $[uv, z] = [u, z]^v[v, z][u, v, z]m$, $m = [v, z, u][v, u, z]^{-1} \in Z(P)$ and $m^2 = 1$, by Lemma 4.1. The element $[u, v, z]$ can be thus expressed as a product of elements from $Z(Q)$ that are of exponent two. Therefore $[u, v, z] = [u, v, z]^u = [v, z, u] = [v, z, u]^v = [z, u, v]$, and we get $[uv, z] = [u, z][v, z][v, u, z]$. We also have $[u, v, z]^z = [z, u, v]^{-1} = [u, v, z]^{-1} = [u, v, z]$, and thus $[u, v, z] \in Z(P)$.

For point (ii) it suffices to note that $[z, z, z] = [z^2, z] = [d, z] = q(d) \in Z(Q)$, and that $[z, z, z]^z = [z, z, z]^{-1} = [z, z, z]$.

For each $u \in Q$, $[z, u, z] = [z, z, u]$, by Lemma 1.4, since $d = z^2 \in N(P)$. If $v \in Q$, then $[z, u, z]^v = [z, u, z][z^2, u, v][z, u, v]^{-2} = [z, u, z]$, by Lemma 1.5 and by point (i) of this proof. This also gives $[z, u, z]^2 = 1$ since $[z, u, z]^u = [z, u, z]^{-1}$, by Lemma 1.4. Furthermore, $[z, uz, z] = [z, z, z]^u[z, u, z] = [z, z, z][z, u, z]$, and $[z, uz, z] = [z, z, z][z, u, z]^z$. Therefore $[z, u, z]^z = [z, u, z]$, and so $[z, u, z] \in Z(P)$. Finally, Lemma 4.1 yields $[d, u] = [z^2, u] = [z, u]^2[z, u, z] = [z, u, z]$. \square

For the next few statements we shall assume that P is as in Proposition 5.1. The associator multiplicative formulas immediately imply:

Corollary 5.2. *Let A be a subloop of P generated by all associators $[\alpha, \beta, \gamma]$ such that $z \in \{\alpha, \beta, \gamma\}$. Then A is a boolean group that is contained in $Z(P)$.*

Corollary 5.3. *Assume $u_i \in Q$ and $\varepsilon_i \in \{0, 1\}$, $1 \leq i \leq 3$. Then*

$$\begin{aligned} [u_1 z^{\varepsilon_1}, u_2 z^{\varepsilon_2}, u_3 z^{\varepsilon_3}] &= [u_1, u_2, u_3][z, u_2, u_3]^{\varepsilon_1}[u_1, z, u_3]^{\varepsilon_2}[u_1, u_2, z]^{\varepsilon_3} \\ &\quad [u_1, z_2, z_3]^{\varepsilon_2 \varepsilon_3}[z_1, u_2, z_3]^{\varepsilon_1 \varepsilon_3}[z_1, z_2, u_3]^{\varepsilon_1 \varepsilon_2}[z_1, z_2, z_3]^{\varepsilon_1 \varepsilon_2 \varepsilon_3}. \end{aligned}$$

Furthermore, $[u_1, u_2, u_3]^z = [u_1, u_2, u_3]$.

Proof. Only the last equality requires a proof. We have $[u_1, u_2, u_3]^z[z, u_2, u_3] = [u_1 z, u_2, u_3] = [u_1, u_2, u_3][z, u_2, u_3]^{u_1} = [u_1, u_2, u_3][z, u_2, u_3]$, by Corollary 5.2. \square

Lemma 5.4. *The loop Q contains normal subloops $A \leq S$ such that $A \leq Z(Q)$, $N(P) \cap Q \leq S$, both A and Q/S are boolean groups, and there exist mappings $q : Q \rightarrow A$ and $\varphi : Q \rightarrow A$ such that:*

- (i) $q(a) = 1$ for all $a \in A(Q)$;
- (ii) $q(u) = q(u') = [z, u]$ whenever $u \equiv u' \pmod{A}$, for all $u, u' \in Q$;
- (iii) $q(du) = q(d)q(u)$ for all $u \in Q$;
- (iv) the mapping $g(u, v) = q(vu)q(u)q(v)$ induces, for all $u, v \in Q$, a group homomorphism $Q/S \rightarrow A$ whenever one of the coordinates is fixed; and
- (v) the mapping $\varphi(u) = [u, d]$ induces a group homomorphism $Q/S \rightarrow A$.

Proof. Let A be defined as in Corollary 5.2. We have $A \leq Z(P) \cap Q \leq Z(Q)$, and A is a boolean group. If $a \in A(Q)$, then $q(a) = [z, a] = [a, z] = a^{-1}a^z$ since $a \in A(P) \leq N(P)$, and $a^z = a$, by Corollary 5.3. This proves point (i).

Point (ii) is clear since $[z, u] = [z, ua]$ for all $u \in Q$ and $a \in A$ as $A \leq Z(P)$, by Corollary 5.2.

We assume $z^2 \in N(P)$, and so $[du, z] = [d, z]^u[u, z] = [d, z][u, z]$, by Lemma 4.1. That gives (iii).

Now, $g(u, v) = [u, v, z]$ for all $u, v \in Q$, by point (i) of Proposition 5.1. The values of $g(u, v) = [u, v, z] \in Z(P)$ depend only upon classes of u and v modulo $N(P)$, and thus $g(u, v) = g(u', v')$ when $u \equiv u' \pmod{N(P)}$ and $v \equiv v' \pmod{N(P)}$. The multiplicative associator formula immediately implies $g(u_1 u_2, v) = g(u_1, v)g(u_2, v)$ and $g(u, v_1 v_2) = g(u, v_1)g(u, v_2)$, for all $u, v, u_1, u_2, v_1, v_2 \in Q$. Similarly, $\varphi(uv) = \varphi(u)\varphi(v)$ for all $u, v \in Q$ since $\varphi(-) = [z, -, z]$, by point (iii) of Proposition 5.1.

We thus have homomorphisms $[z, -, z]$, $[-, u, z]$ and $[u, -, z]$ that map Q into A , where u runs through Q . Since A is a boolean group, Q is a boolean group modulo the kernel of each homomorphism. Therefore it is boolean modulo the intersection

of all kernels, and this intersection gives a subloop $S \geq N(P) \cap Q \geq N(Q)$ that is required by our statement. Points (iv) and (v) thus follow from the earlier computations and from the latter fact. \square

Lemma 5.5. *The following equalities hold for all $u, v \in Q$:*

$$\begin{aligned} zu \cdot v &= z \cdot uv g(u, v), \quad u \cdot zv = z \cdot uv q(u) g(u, v) g(v, u), \\ \text{and } zu \cdot zv &= duv \varphi(v) q(u) g(v, u). \end{aligned}$$

Proof. Indeed, one can compute easily that

$$\begin{aligned} zu \cdot v &= z \cdot uv [z, u, v] = z \cdot uv g(u, v), \\ u \cdot zv &= uz \cdot v [u, z, v] = zu [u, z] \cdot v [u, z, v] = z \cdot uv [u, z] [z, u, v] [u, z, v] \\ &= z \cdot uv q(u) g(u, v) g(v, u), \text{ and} \\ zu \cdot zv &= [z, u] uz \cdot zv = u (z \cdot zv) [z, u] [u, z, zv] = u (z^2 v) [z, z, v] [z, u] [u, z, zv] \\ &= [u, d] duv [d, v] q(u) [u, z, v] [u, d] = duv \varphi(v) q(u) g(v, u). \end{aligned}$$

\square

Our aim now is to show that the properties of the above loop P can be used for a construction based on Q , d and q .

Suppose that Q is a loop with normal subloops A and S . Suppose that d is an element of $N(Q)$, and that $q : Q \rightarrow A$ a mapping. Put $\varphi(u) = [d, u]$ for all $u \in Q$, and $g(u, v) = q(vu)q(u)q(v)$ for all $u, v \in Q$. Assume that

- (1) both A and Q/S are boolean groups, and $A \leq S \cap Z(Q)$;
- (2) $q(ua) = q(u)$ for all $u \in Q$ and $a \in A$;
- (3) $g(u, vw) = g(u, v)g(u, w)$ and $g(vw, u) = g(v, u)g(w, u)$ for all $u, v, w \in Q$;
- (4) $g(us, vt) = g(u, v)$ for all $u, v \in Q$ and $s, t \in S$;
- (5) $\varphi(uv) = \varphi(u)\varphi(v)$ for all $u, v \in Q$;
- (6) $\varphi(us) = \varphi(u)$ for all $u \in Q$ and $s \in S$; and
- (7) $q(du) = q(d)q(u)$ for all $u \in Q$.

Define a loop $P(*) = Q[d, q, z]$ on $Q \cup zQ$, $z \notin Q$, by

$$\begin{aligned} u * v &= uv, & u * zv &= z \cdot uv q(u) g(u, v) g(v, u), \\ zu * v &= zuv g(u, v), & \text{and } zu * zv &= duv \varphi(v) q(u) g(v, u), \end{aligned}$$

for all $u, v \in Q$.

The notation $Q[d, q, z]$ does not carry an identification of subloops A and S . This is not needed, indeed, since A can be replaced by the (central boolean) subgroup generated by all $q(u)$, and S can be replaced by the set of all $x \in Q$ such that $g(u, x) = g(x, u) = 1$ for all $x \in Q$.

The following three lemmas are stated under the assumption that P and Q are as in the above construction.

Lemma 5.6. *Each element of A belongs to $Z(P)$.*

Proof. Consider $u, v \in Q$ and $a \in A$. Then $(u * v) * a = uva = u * (v * a)$, $zu * a = zua$, $zu * (v * a) = z \cdot uvag(u, va) = z \cdot uv g(u, v) a = (zu * v) * a$, $u * (zv * a) = z \cdot uvag(u, va) g(va, u) = z \cdot uv q(u) g(u, v) g(v, u) a = (u * zv) * a$ and $zu * (zv * a) = duv \varphi(va) q(u) g(va, u) = duv \varphi(v) q(u) g(v, u) a = (zu * zv) * a$, which means that a belongs to the right nucleus. Clearly, $zu * a = zua = a * zu$,

and so it remains to show that a also belongs to the left nucleus. This follows from $a * (zu * v) = z \cdot uv g(u, v) a = z \cdot uav g(ua, v) = zua * v = (a * zu) * v$, $a * (u * zv) = (u * zv) * a = ua * zv = (a * u) * zv$ and $a * (zu * zv) = (zu * zv) * a = zua * zv = (a * zu) * zv$. \square

Lemma 5.7. *Let u, v and w be elements of Q . Then*

- (i) $[zu, v, w] = [u, v, w]g(v, w)$,
- (ii) $[u, zv, w] = [v, w, u]g(w, u)$,
- (iii) $[u, v, zw] = [u, v, w]g(u, v)$,
- (iv) $[zu, zv, w] = [u, v, w]\varphi(w)g(w, u)g(v, w)$;
- (v) $[zu, v, zw] = [u, v, w]\varphi(v)g(v, w)g(u, v)$;
- (vi) $[u, zv, zw] = [u, v, w]\varphi(u)g(w, u)g(u, v)$; and
- (vii) $[zu, zv, zw] = [u, v, w]\varphi(d)\varphi(uvw)g(u, v)g(v, w)g(w, u)$.

Proof. Our goal is to compute $[\alpha, \beta, \gamma]$, where $\alpha \in \{u, zu\}$, $\beta \in \{v, zv\}$ and $\gamma \in \{w, zw\}$. By using the definition of $*$ we shall in every case first express $(\alpha * \beta) * \gamma$ as $z^\varepsilon d^\eta (uv \cdot w) a(\alpha, \beta, \gamma)$, where $\varepsilon, \eta \in \{0, 1\}$ and $a = a(\alpha, \beta, \gamma) \in A$. Then we express $\alpha * (\beta * \gamma)$ as $z^\varepsilon d^\eta (u \cdot vw) b(\alpha, \beta, \gamma)$, where $b = b(\alpha, \beta, \gamma) \in A$ again. Now, $[\alpha, \beta, \gamma]$ should be equal to $[u, v, w]c(\alpha, \beta, \gamma)$, with $c = c(\alpha, \beta, \gamma) \in A$. To prove $(\alpha * (\beta * \gamma))[u, v, w]c = (\alpha * \beta) * \gamma$ we hence need to show that $(u \cdot vw)b[u, v, w]c = (uv \cdot w)a$, which amounts to $bc = a$, which is the same as $abc = 1$.

In case (i) we get $(zu * v) * w = z(uv \cdot w)g(u, v)g(uv, w)$ (since $g(uv g(u, v), w) = g(uv, w)$) and $zu * (v * w) = z(u \cdot vw)g(u, vw)$. We have to verify that the product $g(u, v)g(uv, w)g(u, vw)g(v, w)$ vanishes, and that clearly follows from the equality $g(uv, w)g(u, vw) = g(u, w)g(v, w)g(u, v)g(u, w) = g(v, w)g(u, v)$.

To get (ii) compute $(u * zv) * w = z(uv \cdot w)q(u)g(u, v)g(v, u)g(uv, w)$, $u * (zv * w) = z \cdot (u \cdot vw)g(v, w)q(u)g(u, vw)g(vw, u)$ and

$$\begin{aligned} q(u)g(u, v)g(v, u)g(uv, w)g(v, w)q(u)g(u, vw)g(vw, u)g(w, u) = \\ g(u, v)g(v, u)g(u, w)g(u, v)g(u, w)g(v, u) = 1. \end{aligned}$$

For (iii) we get $(u * v) * zw = z \cdot (uv \cdot w)q(uv)g(uv, w)g(w, vu)$, $u * (v * zw) = z \cdot (u \cdot vw)q(v)g(v, w)g(w, v)q(u)g(u, vw)g(vw, u)$ and

$$\begin{aligned} q(uv)g(uv, w)g(w, vu)q(v)g(v, w)g(w, v)q(u)g(u, vw)g(vw, u)g(u, v) = \\ g(v, u)g(u, w)g(w, u)g(u, w)g(v, u)g(w, u)g(v, w) = 1. \end{aligned}$$

To verify (iv) observe that $(zu * zv) * w = d(uv \cdot w)\varphi(v)q(u)g(v, u)$, $zu * (zv * w) = d(u \cdot vw)\varphi(vw)q(u)g(vw, u)g(v, w)$ and

$$\begin{aligned} \varphi(v)q(u)g(v, u)\varphi(vw)q(u)g(vw, u)g(v, w)\varphi(w)g(w, u)g(v, w) = \\ g(v, u)g(v, u)g(w, u)g(v, w)g(w, u)g(v, w) = 1. \end{aligned}$$

Point (v) follows from $(zu * v) * zw = d(uv \cdot w)\varphi(w)q(uv)g(uv, w)g(u, v)$, $zu * (v * zw) = d(u \cdot vw)\varphi(vw)q(u)g(vw, u)q(v)g(v, w)g(w, v)$ and

$$\begin{aligned} \varphi(w)q(uv)g(uv, w)g(u, v)\varphi(vw)q(u)g(vw, u)q(v)g(v, w)g(w, v)\varphi(v)g(v, w)g(u, v) = \\ g(v, u)g(u, w)g(v, w)g(u, v)g(v, u)g(w, u)g(v, w)g(u, v) = 1. \end{aligned}$$

To get (vi) note that $(u * zv) * zw = d(uv \cdot w)\varphi(w)q(uv)g(w, uv)q(u)g(u, v)g(v, u)$, $u * (zv * zw) = d(u \cdot vw)\varphi(u)\varphi(w)q(v)g(w, v)$ and

$$\begin{aligned} & \varphi(w)q(uv)g(w, uv)q(u)g(u, v)g(v, u)\varphi(u)\varphi(w)q(v)g(w, v)\varphi(u)g(w, u)g(u, v) \\ &= g(v, u)g(w, u)g(w, v)g(u, v)g(v, u)g(w, v)g(w, u)g(u, v) = 1. \end{aligned}$$

Finally, $(zu * zv) * zw = zd(uv \cdot w)q(uv)g(uv, w)g(w, uv)\varphi(v)q(u)g(v, u)$, $zu * (zv * zw) = zd(u \cdot vw)\varphi(u)\varphi(w)q(v)g(w, v)g(u, vw)$ and

$$\begin{aligned} & q(uv)g(uv, w)g(w, uv)\varphi(v)q(u)g(v, u)\varphi(u)\varphi(w)q(v)g(w, v)g(u, vw) \\ & \varphi(uvw)g(u, v)g(v, w)g(w, u) = g(v, u)g(u, w)g(v, w)g(w, u)g(w, v) \\ & g(v, u)g(w, v)g(u, v)g(u, w)g(u, v)g(v, w)g(w, u) = 1. \end{aligned}$$

□

Lemma 5.8. *Suppose that $N(Q) \trianglelefteq Q$ and that $Q/N(Q)$ an abelian group. Then $A(P) \leq N(P) \trianglelefteq P$, with $P/N(P)$ an abelian group. Furthermore, $N(Q) \cap S \leq N(P)$.*

Proof. If $x \in N(Q) \cap S$, then $[x, \alpha, \beta] = [\alpha, x, \beta] = [\alpha, \beta, x] = 1$, for all $\alpha, \beta \in P$. This follows directly from Lemma 5.7, by inspecting all possible situations that are described by points (i)-(vi). Hence $N(Q) \cap S \leq N(P(*))$. From Lemma 5.7 we also see that $A(P(*)) \leq N(Q) \cap S$. For the rest of the proof it suffices to find a commutative group $G(*)$ and a homomorphism $f : P(*) \rightarrow G(*)$ such that $N(Q) \cap S$ is equal to the kernel of f .

Put $\bar{Q} = Q/(S \cap N(Q))$. Then \bar{Q} is a commutative group, as both Q/S and $Q/N(Q)$ are assumed to be commutative groups. Define now a loop $G(*)$ on $G = \bar{Q} \cup z\bar{Q}$ by $z\bar{u} * \bar{v} = z \cdot \bar{u}\bar{v}$, $\bar{u} * z\bar{v} = z \cdot \bar{u}\bar{v}$ and $z\bar{u} * z\bar{v} = \bar{d}\bar{u}\bar{v}$. The operation $*$ is clearly commutative. To see that it is associative one can use Lemma 5.6, with \bar{q} and $\bar{\varphi}$ trivial, where $\bar{A} = 1$ and $\bar{S} = S/(S \cap N(Q))$. The mapping f is now defined by $f(u) = \bar{u}$ and $f(zu) = z\bar{u}$. It is clear that this is a homomorphism $P(*) \rightarrow G(*)$ and that $N(Q) \cap S$ is its kernel. □

Lemma 5.9. *Suppose that Q is a Buchsteiner loop such that $q([u, v, w]) = 1$ for all $u, v, w \in Q$. Then P is a Buchsteiner loop as well.*

Proof. The conditions of Lemma 5.8 are satisfied and hence we know that $A(P(*)) \leq N(P(*)) \trianglelefteq P(*)$. Therefore we only need to prove that $[\alpha, \beta, \gamma]^\alpha = [\beta, \gamma, \alpha]^{-1}$, for all $\alpha, \beta, \gamma \in P$. If $x \in Q$, then $z \setminus (xz) = xq(x)$, by the definition of P . Thus $[u, v, w]^z = [u, v, w]$ for all $u, v, w \in Q$, by assumptions of the lemma. The right hand sides of all equalities in Lemma 5.7 are hence invariant under the action of z . This means that we need to verify $[\alpha, \beta, \gamma]^u = [\beta, \gamma, \alpha]^{-1}$ for all cases when $\alpha \in \{u, zu\}$, $\beta \in \{v, zv\}$ and $\gamma \in \{w, zw\}$. Now, $[\alpha, \beta, \gamma]^u = [u, v, w]^u c(\alpha, \beta, \gamma)$ for some $c(\alpha, \beta, \gamma) \in A$, and $[\beta, \gamma, \alpha]^{-1} = [v, w, u]^{-1} c(\beta, \gamma, \alpha)$. Since we assume $[u, v, w]^u = [v, w, u]^{-1}$, we have to show that $c(\beta, \gamma, \alpha) = c(\alpha, \beta, \gamma)$, for all cases (i)-(vii) of Lemma 5.6. Now, indeed $c(v, w, zu) = g(v, w)$, $c(zv, w, u) = g(w, u)$, $c(v, zw, u) = g(u, v)$, $c(zv, w, zu) = \varphi(w)g(w, u)g(v, w)$, $c(v, zw, zu) = \varphi(v)g(u, v)g(v, w)$, $c(zv, zw, u) = \varphi(u)g(u, v)g(w, u)$, and the last case is clear since it is cyclically invariant. □

We are now ready for the final statements of this section.

Proposition 5.10. *Let Q be a Buchsteiner loop with normal subloops A and S , and with an element $d \in N(Q)$. Furthermore, let $q : Q \rightarrow A$ be a mapping such that $q(a) = 1$ for all $a \in A(Q)$, and let z be an element outside Q . If d and q satisfy conditions (1)–(7), then $P = Q[d, q, z]$ is a Buchsteiner loop with $A \leq Z(P)$, $A(P) \leq N(Q) \cap S \leq N(P)$ and $N(Q) \cap S \leq N(P)$, where $P/N(Q) \cap S$ is an abelian group.*

If Q is a conjugacy closed loop, then $[\alpha, \beta, \gamma] = [\beta, \gamma, \alpha]$ for all $\alpha, \beta, \gamma \in P$. In such case P is conjugacy closed if and only if $g(u, v) = g(v, u)$ for all $u, v \in Q$.

Proof. Use Lemmas 5.6, 5.8 and 5.9.

Proposition 5.11. *Let P be a Buchsteiner loop that contains a normal subloop Q , $|P : Q| = 2$, and an element $z \in P \setminus Q$ such that $d = z^2 \in N(P)$, and $[z, u]$ is a central element of Q , $[z, u]^2 = 1$, for all $u \in Q$. Set $q(u) = [z, u]$ for all $u \in Q$. Then $P = Q[d, q, z]$.*

Proof. This is just another expression of Lemma 5.5. \square

6. PROPER BUCHSTEINER LOOPS OF ORDER 32

We shall first show that such loops really exist, by applying the doubling construction of Section 5 to the group $Q = G \times A$, where G is a group of quaternions and A is a two-element group. The (only) natural choice for S is the subgroup $G' \times A$. The mapping $q : Q \rightarrow A$ has to depend only upon the elements of G (by condition (2)), and so we shall be looking for a mapping $q : G \rightarrow \{0, 1\}$ such that $g(u, v) = q(vu) + q(u) + q(v)$ yields a bilinear mapping $G/G' \rightarrow \{0, 1\}$. If q is such a mapping, then we can always set $d = 1$, and that gives a Buchsteiner loop P , by Proposition 5.10. However, the loop P might be conjugacy closed. To avoid this case we need to make sure that $g(-, -)$ is not symmetric (see Proposition 5.10 again).

Lemma 6.1. *Let G be a group of quaternions generated by elements x, y and z such that $xy = z$, $yz = x$ and $zx = y$. Let $s = x^2 = y^2 = z^2$ be the only nontrivial square of G . Define $q : G \rightarrow \{0, 1\}$ in such a way that $q(u) = 1$ if and only if $u \in \{s, x, y, z\}$. Then G/G' is a vector space over $\{0, 1\}$, and the mapping $g : G \times G \rightarrow \{0, 1\}$, $(u, v) \rightarrow q(vu) + q(u) + q(v)$, induces a non-symmetric bilinear form on G/G' .*

Proof. We see that $q(us) = q(s) + q(u)$ for all $u \in G$. The element s is central and so $g(u, v)$ clearly does not change if u is replaced by us or v by vs . If u and v generate G , then $s = [u, v]$, and $g(u, v) = g(v, u) + 1$. For the proof it therefore suffices to show that $g(u, vw) = g(u, v) + g(u, w)$, where $u, v, w \in \{x, y, z\}$ and $vw \in \{s, x, y, z\}$. The case $v = w$ is clear, and so $v \neq w$ can be assumed. We can also assume $u = x$ because $\text{Aut}(G)$ acts transitively upon $\{x, y, z\}$. Now $g(x, xy) = g(x, z) = q(zx) = 1 = g(x, x) = g(x, x) + g(x, y)$, $g(x, zx) = 0 = g(x, x) + g(x, z)$, and $g(x, yz) = g(x, x) = 1 = g(x, z) = g(x, y) + g(x, z)$. \square

Corollary 6.2. *There exists a proper Buchsteiner loop of order 32.*

Proof. Indeed, set $P = Q[q, 1, z]$, with $Q = G \times A$, $G \cong Q_8$, $A \cong C_2$, $z \notin Q$, and $q(ua) = 1$, where $u \in G$ and $a \in A$, if and only if $u \in \{1, x^{-1}, y^{-1}, yx\}$, for some generators x and y of G . \square

Theorem 6.3. *Let P be a proper Buchsteiner loop of order 32. Then $1 < A(P) < N(P) < Z_2(P)$, $|Z_2(P)| = 8$, $A(P) = Z(P)$ and there exists a unique power associative conjugacy closed subloop Q of index two such that $QZ_2(P) = P$ and $Q \cap Z_2(P) = N(P) = Z(Q)$. The group $Q/A(P)$ is noncommutative.*

Proof. Set $A = A(P)$ and $N = N(P)$. We have $A = P$, $|A| = 2$ and $|N| = 4$, by Proposition 4.8. Set also $C = Z_2(P)$. The subloop C consists of all elements that are central modulo A . Group $H = P/A$ is nonabelian, and group P/N is elementary abelian of order 8, again by Proposition 4.8. The group H thus contains a two-element subgroup modulo which it is a vector space of dimension 3, and the square mapping induces a quadratic form of the vector space into this subgroup. The radical of this quadratic form corresponds to $Z(H)$, and so $|Z(H)| = 4$. The preimage of $Z(H)$ modulo A is equal to C , the second centre of P . If $x \in Q$ and $c \in C$, then $[x, c] \in Z = A$, and $[xy, c] = [x, c][y, c][y, x, c]$, by Lemma 4.1. Furthermore, $[c, u] = [u, c]$ and $[u, c]^2 = 1$, since A has only two elements. Clearly, $c^2 \in N$.

Consider the action of $H = P/A$ upon N , $n \mapsto x \backslash (nx)$. This action has to be nontrivial since $A = Z$, and $|N : A| = 2$. However, each element of H acts trivially upon A , and so the image of the action contains exactly two permutations (the identity and the transposition of elements of $N \setminus A$). The kernel of this action is hence a subgroup of H that is of index two. The preimage of the kernel in H is a subloop Q , and this subloop satisfies $Z(Q) \geq N$. Note that P contains exactly one such subloop of index two since each element of Q acts trivially upon N .

We shall be now establishing the properties of Q . It is clear that Q is conjugacy closed, by Proposition 4.8. Choose $x, y, z \in P$ so that they form a basis modulo N , and $z \in C$. From Corollary 2.5 we see that these elements generate Q . The associator $[x, y, z]$ is central, and hence invariant under cyclic shifts, by Lemma 4.2. Therefore $[x, y, z] \neq [y, x, z]$, by Lemma 2.3, and hence $[xy, z] \neq [yx, z]$, by the formula $[xy, z] = [x, c][y, c][y, x, c]$. Now, the same formula gives $[xy, z] = [yx[x, y], z] = [yx, z][[x, y], z]$, and so we see that z acts nontrivially upon $[x, y] \in N$. That means that z cannot belong to Q . Thus $N = Q \cap C$. In fact, we have shown even more, since for each $x \in Q \setminus N$ we can find $y \in Q$ such that x, y, z is a basis modulo N , and so for each $x \in Q \setminus N$ there exists $y \in Q$ with $[x, y] \neq 1$. Hence $Z(Q) = N$. The loop Q is power associative since $x^2 \in Z(Q)$ for all $x \in Q$. \square

Corollary 6.4. *Each proper Buchsteiner loop of order 32 can be obtained by the doubling construction.*

7. ABELIAN INNER MAPPINGS GROUPS

We start by applying well known facts about inner mappings to Buchsteiner loops.

Lemma 7.1. *Let Q be a Buchsteiner loop such that $A(Q) \leq N(Q)$. Then*

$$L(x, y)(z) = z[x, y, z]^{-1}, \quad R(x, y)(z) = z[y, x, z], \quad \text{and} \quad T_x^{-1}(z) = z[z, x],$$

for all $x, y, z \in Q$.

Proof. Recall that $(x \cdot yz)[x, y, z] = xy \cdot z$. This means $(x \cdot yz) = xy \cdot (z[x, y, z]^{-1})$, since $[x, y, z] \in N(Q)$, and so $L(x, y)(z) = z[x, y, z]^{-1}$. Now $(z \cdot yx)[z, y, x] = zy \cdot x = (((z \cdot yx)[z, y, x]) / (z \cdot yx))(z \cdot yx) = [z, y, x]^{(zyx)^{-1}}(z \cdot yx) = [z, y, x]^{x^{-1}y^{-1}z^{-1}}(z \cdot yx) =$

$[y, x, z]^{z^{-1}}(z \cdot yx) = (((z[y, x, z])/z)z) \cdot yx = z[y, x, z] \cdot yx$. Hence $R(x, y)(z) = z[y, x, z]$. To prove $x \setminus (zx) = z((xz) \setminus (zx))$ it suffices to multiply the equality by x on the left, and to use the fact that $[z, x] = (xz) \setminus (zx)$ belongs to the nucleus. \square

Lemma 7.2. *Let Q be a Buchsteiner loop. Then the set of all $L(x, y)$ and $R(x, y)$ generates an abelian group, and this group belongs to the center of $\text{Inn } Q$ if and only if $A(Q) \leq Z(Q)$.*

Proof. Clearly, $R(x, y)R(u, v)(z) = R(x, y)(z[v, u, z]) = z[v, u, z][y, x, z[v, u, z]] = z[v, u, z][y, x, z]$, and the other cases are similar (in fact, their inspections is not needed when one takes in account that $\mathcal{L}_1 = \mathcal{R}_1$, in every Buchsteiner loop Q). Now, $R(x, y)T_u^{-1}(z) = R(x, y)(z[z, u]) = z[z, u][y, x, z[z, u]] = z[z, u][y, x, z]$, and $T_u^{-1}R(x, y)(z) = T_u^{-1}(z[y, x, z]) = z[y, x, z][z[y, x, z], u]$. Set $a = [y, x, z]$ and note that $a \in Z(N)$, and that $[za, u] = [z, u][a, u]$, by Lemma 4.1. Hence $R(x, y)$ and T_u commute for all $x, y, u \in Q$ if and only if $[a, u] = 1$ for all $a \in A(Q)$. This is the same as to say that $A(Q) \leq Z(Q)$. \square

Proposition 7.3. *Let Q be a Buchsteiner loop with $A(Q) \leq Z(Q)$. Then both Q/N and $A(Q)$ are boolean groups and $[x, y, z] = [y, z, x]$ for all $x, y, z \in Q$. If $A(Q)$ is not a central subloop of Q , then $\text{Inn } Q$ is not an abelian group. If $A(Q) \leq Z(Q)$, then $\text{Inn } Q$ is abelian if and only if*

$$[z, u][z, v]^u = [z, v][z, u]^v \text{ or, equivalently, } [z, vu][z, v, u] = [z, uv][z, u, v],$$

for all $u, v, z \in Q$.

Proof. If $\text{Inn } Q$ is abelian, then $A(Q) \leq Z(Q)$, by Lemma 7.2. Assume $A(Q) \leq Z(Q)$. Then Q/N and $A(Q)$ are boolean groups, and the associators are cyclically invariant, by Lemma 4.2. In light of Lemma 7.2 it is clear that if $A(Q) \leq Z(Q)$, then $\text{Inn } Q$ is abelian if and only if the mappings $z \mapsto z[z, u]$ and $z \mapsto z[z, v]$ commute, for all $u, v \in Q$. This gives us the equality

$$z[z, u][z[z, u], v] = z[z, v][z[z, v], u], \text{ for all } u, v, z \in Q.$$

By Lemma 4.1, $[z, u][z[z, u], v] = [z, u][z, v]^{[z, u]}[[z, u], v] = [z, v][z, u][[z, u], v]$. Hence

$$[z, v][z, u][[z, u], v] = [z, u][z, v][[z, v], u]$$

is a condition that expresses the commutativity of the above mappings.

We have $[x, y] = [y, x]^{-1}$, since $[x, y] \in N(Q)$, for all $x, y \in Q$. From Lemma 4.1 we hence get the general equality

$$[z, xy] = [z, y][z, x]^y[z, y, x], \text{ for all } x, y, z \in Q.$$

Now, $[z, v][z, u][[z, u], v] = [z, v][z, u][z, u]^{-1}[z, u]^v = [z, v][z, u]^v = [z, uv][z, v, u]$, and the rest is clear. \square

For a loop Q one can define Q' in a similar way as in groups, i.e. as the least normal subloop S such that Q/S is an abelian group. If $N(Q) \leq Q$ and $Q/N(Q)$ is abelian, then clearly $Q' \leq N(Q)$. This is so in every Buchsteiner loop Q , and hence Q' has to be always a group in such loops. Note, that Lemma 4.1 can be used to see that Q' coincides with the subloop generated by all associators $[x, y, z]$ and commutators $[x, y]$.

Lemma 7.4. *Let Q be a Buchsteiner loop with $\text{Inn } Q$ abelian. Then Q' is abelian as well.*

Proof. Consider $x, y_1, y_2, z \in Q$ and put $y = y_1 y_2$. Then $[z, y_1 y_2]$ is equal to $[z, y_2][z, y_1]^{y_2}[z, y_2, y_1]$, and so $[z, y][z, x]^y = [z, x][z, y]^x$ gives

$$[z, y_2][z, y_1]^{y_2}[z, x]^{y_1 y_2} = [z, x][z, y_2]^x[z, y_1]^{y_2 x} = [z, y_2][z, x]^{y_2}[z, y_1]^{y_2 x}.$$

We also have $[z, y_1]^{y_2}[z, x]^{y_1 y_2} = [z, x]^{y_2}[z, y_1]^{x y_2}$, and that means that $[z, y_1]^{y_2 x} = [z, y_1]^{x y_2}$. In other words, $[u_1, u_2]^{vw} = [u_1, u_2]^{wv}$ for all $u_1, u_2, v, w \in Q$. That is the same as $[u_1, u_2]^{[v, w]} = [u_1, u_2]$, and so $[u_1, u_2][v, w] = [v, w][u_1, u_2]$. Each commutator and each associator thus commutes with every commutator and with every associator. The group Q' is hence abelian. \square

Let Q be a Buchsteiner loop. Then $Q/A(Q)$ acts upon $N(Q)$, and so also upon Q' . If Q' is abelian, then we get an action of Q/Q' upon Q' , and so we get an action of an abelian group upon an abelian group. We shall use this fact freely in the following lemma, understanding that $T_x^{-1}([u, v]) = [u, v]^x$ means in fact the action of xQ' upon $[u, v]$, and so $[u, v]^{yx} = [u, v]^{yx}$, for all $x, y \in Q$.

Lemma 7.5. *Let Q be a Buchsteiner loop with $A(Q) \leq Z(Q)$ and Q' abelian that is generated by a set X . If $[z, y][z, x]^y = [z, x][z, y]^x$ holds for all $x, y, z \in X$, then it holds for all $x, y, z \in Q$.*

Proof. Let us have $y = y_1 y_2$, where $y_1, y_2 \in Q$. We can express $[z, y_1 y_2]$ as $[z, y_2][z, y_1]^{y_2}[z, y_2, y_1]$, and we see that $[z, y][z, x]^y$ equals $[z, x][z, y]^x$ if and only if $[z, y_2][z, y_1]^{y_2}[z, x]^{y_1 y_2}$ equals $[z, x][z, y_2]^x[z, y_1]^{y_2 x}$. The equality thus takes place if and only if $a = b^{y_2}$, where $a = ([z, x][z, y_2]^x)^{-1}[z, y_2][z, x]^{y_2}$ and $b = [z, y_1]^x([z, x]^{y_1}[z, y_1])^{-1}[z, x]$. Hence

$$\begin{aligned} a = b^{y_2} &\Leftrightarrow [z, y][z, x]^y = [z, x][z, y]^x, \\ a = 1 &\Leftrightarrow [z, y_2][z, x]^{y_2} = [z, x][z, y_2]^x, \text{ and} \\ b = 1 &\Leftrightarrow [z, y_1][z, x]^{y_1} = [z, x][z, y_1]^x. \end{aligned}$$

(Note that we have been using the commutativity of Q' when expressing the condition $b = 1$). If two of conditions $a = b^{y_2}$, $a = 1$ and $b = 1$ are true, then the third one is true as well. From that we see that if $[z, u_i][z, x]^{u_i} = [z, x][z, u_i]^x$ holds for $i \in \{1, 2\}$, then $[z, u][z, x]^u = [z, x][z, u]^x$ for every $u \in \{u_1 u_2, u_1/u_2, u_1 \setminus u_2\}$.

The case $z = z_1 z_2$ is similar. We have $[z_1 z_2, y][z_1 z_2, x]^y = [z_1 z_2, x][z_1 z_2, y]^x$ if and only if $[z_1, y]^{z_2}[z_2, y][z_1, x]^{z_2 y}[z_2, x]^y$ equals $[z_1, x]^{z_2}[z_2, x][z_1, y]^{z_2 x}[z_2, y]^x$. The equality takes place if and only if $a^{z_2} = b$, where $a = [z_1, y][z_1, x]^y([z_1, x][z_1, y]^x)^{-1}$ and $b = [z_2, x][z_2, y]^x([z_2, y][z_2, x]^y)^{-1}$. The rest is clear. \square

8. CONSTRUCTION OF A BUCHSTEINER LOOP OF ORDER 128

The purpose of this section is to show that there exist proper Buchsteiner loops with $\text{Inn } Q$ abelian. Such loops cannot be of nilpotency class two, since then they would be conjugacy closed, by Corollary 4.4.

We shall be constructing a loop Q with $N(Q) = Q'$, $Q/Q' \cong C_2 \times C_2 \times C_2$ and $Q' \cong C_4 \times C_2 \times C_2$. The loop will be defined by a traditional method upon the set

$B \times N$, where $B \cong Q/Q'$ is written multiplicatively and $N \cong N(Q)$ additively, B acts multiplicatively upon N , and

$$(u, a) \cdot (v, b) = (uv, \theta(u, v) + va + b) \text{ for all } u, v \in B \text{ and } a, b \in N,$$

where the factor system (2-cocycle) $\theta : B \times B \rightarrow N$ is defined in such a way that $\theta(u, 1) = 0 = \theta(1, u)$ for all $u \in B$.

For loops defined in this way (with both B and N abelian) one can easily compute the associator $[(u, a), (v, b), (w, c)]$ as

$$(1, \theta(uv, w) + w\theta(u, v) - \theta(u, vw) - \theta(v, w)),$$

which means that $1 \times B$ is always contained in the nucleus (and thus also in the commutant).

Assume that B is generated by e_i , $1 \leq i \leq 3$, and that N is generated by h , an element of order four, and by a subgroup $\{0, c_1, c_2, c_3\}$ that is isomorphic to $C_2 \times C_2$. We shall write $2h$ sometimes as d , and so $-h = d + h$.

Define a (multiplicative) action of B upon N by

$$e_i h = h + d, \quad e_i c_i = c_i \text{ and } e_i c_j = c_j + d,$$

for all $i, j \in \{1, 2, 3\}$, $i \neq j$. Clearly, $ud = d$, for all $u \in B$, and B acts trivially upon N/D , $D = \{0, d\}$.

We shall define $\theta : B \times B \rightarrow N$ as a sum, with $\theta(u, v) = \eta(u, v) + \delta(u, v)d$ for all $u, v \in B$, where $\eta : B \times B \rightarrow N$, and $\delta : B \times B \rightarrow \{0, 1\}$. Now,

$$\eta(\prod e_i^{\alpha_i}, \prod e_i^{\beta_i}) = \sum \alpha_i \beta_{i-1} h + \sum (\alpha_i \beta_i + \alpha_{i-1} \beta_{i+1}) c_i,$$

where $\alpha_i, \beta_i \in \{0, 1\}$, and the indices are computed modulo three. Furthermore,

$$\delta(\prod e_i^{\alpha_i}, \prod e_i^{\beta_i}) = \sum \alpha_i \alpha_{i+1} \beta_i + \sum (\alpha_i + \alpha_{i-1}) \beta_i \beta_{i+1},$$

again for all $\alpha_i, \beta_i \in \{0, 1\}$ (the indices are computed modulo three, and the expression is computed modulo two).

The mapping η is defined so that $\eta(e_i, e_i) = c_i$, $\eta(e_i, e_{i+1}) = 0$ and $\eta(e_i, e_{i-1}) = h + c_{i+1}$.

Lemma 8.1. *Assume $\alpha_i, \beta_j \in \{0, 1\}$, $i, j \in \{1, 2, 3\}$. Then*

$$\eta(\prod e_i^{\alpha_i}, \prod e_j^{\beta_j}) = \sum \alpha_i \beta_j \eta(e_i, e_j).$$

Proof. We have $\sum \alpha_i \beta_j \eta(e_i, e_j) = \sum \alpha_i \beta_i c_i + \sum \alpha_i \beta_{i-1} (h + c_{i+1}) = \sum \alpha_i \beta_{i-1} h + \sum (\alpha_i \beta_i + \alpha_{i-1} \beta_{i+1}) c_i$. \square

Lemma 8.1 seems to suggest that $h(uv, w) = h(u, w) + h(v, w)$ and $h(w, uv) = h(w, u) + h(w, v)$, for all $u, v, w \in B$. However, none of these two equalities holds in general. The reason is that B is of exponent two and $\eta(e_i, e_{i-1})$ is an element of order four. Nevertheless, it is not difficult to compute the correction terms. For that we shall use \oplus as the addition modulo 2 upon $\{0, 1\}$. Note that for $\alpha, \beta \in \{0, 1\}$ we always have $\alpha \oplus \beta = \alpha + \beta - 2\alpha\beta$, where the addition on the right hand side is that of integers.

Lemma 8.2. *Let $u = \prod e_i^{\alpha_i}$, $v = \prod e_i^{\beta_i}$ and $w = \prod e_i^{\gamma_i}$ be elements of B . Then*

$$\begin{aligned} \eta(uv, w) - \eta(u, w) - \eta(v, w) &= (\sum \alpha_{i+1} \beta_{i+1} \gamma_i) d, \text{ and} \\ \eta(u, vw) - \eta(u, v) - \eta(v, w) &= (\sum \alpha_{i+1} \beta_i \gamma_i) d. \end{aligned}$$

Proof. Set first $\lambda_i = \alpha_i + \beta_i - 2\alpha_i\beta_i = \alpha_i \oplus \beta_i$, $1 \leq i \leq 3$. Then $uv = \prod e_i^{\lambda_i}$, and $\eta(uv, w) = \sum \lambda_i \gamma_{i-1} h + \sum (\lambda_i \gamma_i + \lambda_{i-1} \gamma_{i+1}) c_i = \sum (\alpha_i \beta_i \gamma_{i-1}) d + \sum (\alpha_i \gamma_{i-1} + \beta_i \gamma_{i-1}) h + \sum (\alpha_i \gamma_i + \beta_i \gamma_i + \alpha_{i-1} \gamma_{i+1} + \beta_{i-1} \gamma_{i+1}) c_i$, and that makes the former equality clear. For the latter one proceed similarly, set $\nu_i = \beta_i + \gamma_i - 2\beta_i \gamma_i$ and note that $\alpha_i \nu_{i-1} h = (\alpha_i \beta_i + \alpha_i \gamma_i) h + \alpha_i \beta_{i-1} \gamma_{i-1}$. \square

To be able to utilize Lemma 8.2 in the computation of the associator we need to be able to express the difference of $w\eta(u, v)$ and $\eta(uv)$. This is the content of the next lemma.

Lemma 8.3. *Let $u = \prod e_i^{\alpha_i}$, $v = \prod e_i^{\beta_i}$ and $w = \prod e_i^{\gamma_i}$ be elements of B , and let $x = \lambda h + \sum \rho_j c_j$ be an element of N . Then $wx - x = \sum \gamma_i (\lambda + \rho_{i-1} + \rho_{i+1}) d$ and*

$$w\eta(u, v) - \eta(u, v) = \sum (\alpha_{i-1} \beta_{i-1} + \alpha_{i+1} \beta_{i+1} + \alpha_{i-1} \beta_{i+1}) \gamma_i d.$$

Proof. First note that the formula for $wx - x$ is defined correctly. Indeed, set $\rho'_i = \rho_i + \rho_3$ for $i \in \{1, 2\}$ and set $\rho'_3 = 0$. Then $(\rho_{3-1} + \rho_{3+1})d = (\rho'_{3-1} + \rho'_{3+1})d$ and for $i \in \{1, 2\}$ we get $\rho_{i-1} + \rho_{i+1} = \rho'_{i-1} + \rho'_{i+1}$. The mapping $x \mapsto \sum \gamma_i (\lambda + \rho_{i-1} + \rho_{i+1}) d$ thus yields an endomorphism of the abelian group N . The mapping $x \mapsto wx - x$ is also such an endomorphism, and hence it suffices to verify that both endomorphisms agree for $x = h$ and $x = c_j$. However, that comes immediately from the definition of the action of B upon N .

We have to apply the endomorphism to $x = \eta(u, v)$, which means that $\lambda = \sum \alpha_i \beta_{i-1}$ and $\rho_j = \alpha_j \beta_j + \alpha_{j-1} \beta_{j+1}$. Each $\gamma_j d$ is hence multiplied by $\alpha_j \beta_{j-1} + \alpha_{j-1} \beta_{j+1} + \alpha_{j+1} \beta_j + \alpha_{j-1} \beta_{j-1} + \alpha_{j+1} \beta_j + \alpha_{j+1} \beta_{j+1} + \alpha_j \beta_{j-1}$, and that is equal modulo 2 to $\alpha_{j-1} \beta_{j+1} + \alpha_{j-1} \beta_{j-1} + \alpha_{j+1} \beta_{j+1}$, for all $j \in \{1, 2, 3\}$. \square

Corollary 8.4. *Let $u = \prod e_i^{\alpha_i}$, $v = \prod e_i^{\beta_i}$ and $w = \prod e_i^{\gamma_i}$ be elements of B . Then $\eta(uv, w) + w\eta(u, v) - \eta(u, vw) - \eta(v, w)$ is equal to $\sum (\alpha_{i-1} \beta_{i-1} + \alpha_{i-1} \beta_{i+1} + \alpha_{i+1} \beta_i) \gamma_i d$.*

Lemma 8.5. *Let $u = \prod e_i^{\alpha_i}$, $v = \prod e_i^{\beta_i}$ and $w = \prod e_i^{\gamma_i}$ be elements of B . Then $\delta(u + v, w) + \delta(u, v) + \delta(u, v + w) + \delta(v, w)$ is modulo 2 equal to $\sum (\alpha_{i-1} \beta_{i-1} + \alpha_{i-1} \beta_{i+1} + \alpha_{i+1} \beta_i + \alpha_{i+1} \beta_{i-1}) \gamma_i$.*

Proof. By definition,

$$\delta(u + v, w) = \sum (\alpha_i + \beta_i)(\alpha_{i+1} + \beta_{i+1}) \gamma_i + \sum (\alpha_i + \alpha_{i-1} + \beta_i + \beta_{i-1}) \gamma_i \gamma_{i+1},$$

which is clearly equal to $\delta(u, w) + \delta(v, w) + \sum (\alpha_i \beta_{i+1} + \alpha_{i+1} \beta_i) \gamma_i$. Similarly,

$$\delta(u, v + w) = \sum \alpha_i \alpha_{i+1} (\beta_i + \gamma_i) + \sum (\alpha_{i-1} + \alpha_i) (\beta_i + \gamma_i) (\beta_{i+1} + \gamma_{i+1})$$

is equal to $\delta(u, v) + \delta(u, w) + \sum (\alpha_{i-1} + \alpha_i) (\beta_i \gamma_{i+1} + \beta_{i+1} \gamma_i)$, and the latter sum can be clearly expressed also as $\sum (\alpha_{i-1} \beta_{i+1} + \alpha_i \beta_{i+1} + \alpha_{i+1} \beta_{i-1} + \alpha_{i-1} \beta_{i-1}) \gamma_i$. The rest is obvious. \square

Proposition 8.6. *The loop Q is a Buchsteiner loop that is not conjugacy closed. It is of nilpotency class three and its inner mapping group is abelian. The nucleus of Q is equal to $1 \times N$ and coincides with Q' , the centre is equal to $\{(1, 0), (1, d)\}$ and coincides with $A(Q)$. Finally, $Z(Q/Z(Q)) = N(Q)/Z(Q)$.*

Proof. Let $u = \prod e_i^{\alpha_i}$, $v = \prod e_i^{\beta_i}$ and $w = \prod e_i^{\gamma_i}$ be elements of B . The associator is given by $\theta(uv, w) + w\theta(u, v) - \theta(u, vw) - \theta(v, w)$ which equals the sum $\eta(uv, w) + w\eta(u, v) - \eta(u, vw) - \eta(v, w)$ and of $(\delta(uv, w) + \delta(u, v) + \delta(u, vw) + \delta(v, w))d$ since $w\theta(u, v) = w\eta(u, v) + \delta(u, v)d$. From Corollary 8.4 and Lemma 8.5 we hence get

$$[u, v, w] = (1, \sum \alpha_{i+1}\beta_{i-1}\gamma_i)d = (1, \sum \alpha_{i-1}\beta_i\gamma_{i+1})d.$$

Loop Q has to be a Buchsteiner loop since $[u, v, w] = [v, w, u] = [w, v, u]$ is a central element of exponent 2, for all $u, v, w \in Q$. If e_i is identified with $(e_i, 0)$, and $(1, a)$ with a , for all $a \in N$, then we get $[e_1, e_2, e_3] = d$, $[e_1, e_3, e_2] = 0$, and the other associator values can be computed by cyclic shifts and by linearity.

One needs to multiply $(v, b) \cdot (u, b) = (vu, \theta(v, u) + ub + a)$ by $(0, \theta(u, v) - \theta(v, u) + (v - 1)a + (1 - u)b)$ to get $(u, a) \cdot (v, b) = (uv, \theta(u, v) + va + b)$. Thus $[e_i, e_j] = \theta(e_i, e_j) - \theta(e_j, e_i)$, and we get

$$[e_i, e_{i+1}] = h + d + c_{i-1} \text{ and } [e_i, e_{i-1}] = h + c_{i+1}.$$

Furthermore, $[e_i e_{i+1}, e_{i-1} e_i] = \eta(e_i e_{i+1}, e_i e_{i-1}) - \eta(e_i e_{i-1}, e_i e_{i+1}) = (d + c_i + c_{i+1} + c_{i-1}) - h = h$. It is hence clear that Q' is equal to $N(Q) = 1 \times N$. To see that $Z(Q/Z(Q)) = N(Q)/Z(Q)$ it remains to verify that $(e_1 e_2 e_3, 0)$ does not commute with all elements of Q modulo $Z(Q)$. However, $\theta(e_1, e_1 e_2 e_3) - \theta(e_1 e_2 e_3, e_1) = (h + c_3) - (h + c_2 + d) = d + c_1 \notin Z(Q)$.

To finish the proof we need to show that $[e_i, e_k] + e_i[e_j, e_k] = [e_j, e_k] + e_j[e_i, e_k]$ for all $i, j, k \in \{1, 2, 3\}$, by Lemma 8.4. The case $i = j$ is trivial, and so we can assume $j = i + 1$, by the symmetry of i and j . If $k = i$, then $e_i[e_{i+1}, e_i] = e_i(h + c_{i-1}) = h + c_{i-1} = [e_{i+1}, e_i]$. If $k = j = i + 1$, then $[e_i, e_{i+1}] = h + d + c_{i-1} = e_{i+1}[e_i, e_{i+1}]$. Finally, let us have $k = i - 1$. Then $[e_i, e_{i-1}] + e_i[e_{i+1}, e_{i-1}] = (h + c_{i+1}) + e_i(h + d + c_i) = d + c_{i-1} = (h + d + c_i) + e_{i+1}(h + c_{i+1}) = [e_{i+1}, e_{i-1}] + e_{i+1}[e_i, e_{i-1}]$. \square

REFERENCES

- [1] R. H. Bruck: Contributions to the theory of loops, *Trans. Amer. Math. Soc.* **60** (1946), 245–354.
- [2] H. H. Buchsteiner: O nektorom klasse binarnych lup, *Mat. Issled.* **39** (1976), 54–66.
- [3] P. Csörgő and A. Drápal: Left conjugacy closed loops of nilpotency class two, *Results Math.* **47** (2005), 242–265.
- [4] P. Csörgő: On connected transversals to abelian subgroups and loop theoretical consequences, *Arch. Math. (Basel)* **86** (2006), 499–516.
- [5] P. Csörgő: Abelian inner mappings and nilpotency class greater than two, *Europ. J. Comb.* **28** (2007), 858–868.
- [6] P. Csörgő and A. Drápal: Loops that are conjugacy closed modulo the center (submitted).
- [7] P. Csörgő and A. Drápal: Buchsteiner loops and conjugacy closedness (submitted).
- [8] P. Csörgő, A. Drápal and M. Kinyon: Buchsteiner loops (submitted).
- [9] A. Drápal, P. Jedlička: On loop identities that can be obtained by a nuclear identification (submitted).
- [10] M. K. Kinyon, K. Kunen, J. D. Phillips: Diassociativity in conjugacy closed loops, *Comm. Algebra* **32** (2004), 767–786.
- [11] M. K. Kinyon, K. Kunen: Power-associative, conjugacy closed loops, *J. Algebra* **304** (2006), 269–294.

DEPT. OF MATHEMATICS, CHARLES UNIVERSITY, SOKOLOVSKÁ 83, 186 75 PRAHA 8, CZECH REP.

E-mail address: drapal@karlin.mff.cuni.cz

DEPT. OF MATHEMATICS, UNIVERSITY OF DENVER, 2360 S. GAYLORD ST., DENVER, COLORADO
80208, U.S.A.

E-mail address: `mkinyon@math.du.edu`